LJN'S
# Product Liability
Law & Strategy®

LAW JOURNAL NEWSLETTERS

An incisivemedia publication

Volume 28, Number 5 • November 2008

## Whose Space? Discovery of Social Networking Web Sites

**By Ronald J. Levine and Susan L. Swatski-Lebson**

Peggy casually sits at her work station writing in her "MyFazer" (a fictional name of a social networking site). She is reporting on the backyard party she attended over the weekend. She reminisces about the fun she had bouncing on a trampoline with the entire football team before it collapsed. She ponders — Could her resulting injuries be her "golden ticket" to escape from a mountain of debt? Could she now force her employer, INC, to give her a prime office on the first floor and a front-line parking space?

Shortly thereafter, Peggy files suit against the manufacturer of the trampoline. She also advises INC that she sustained a serious injury that dramatically inhibited her mobility and rendered her in need of a workplace "accommodation."

During discovery, counsel for the trampoline manufacturer demands production of any and all communications about or relating to the incident, including any responsive entries on Peggy's MyFazer page. Peggy's counsel refuses to supply the demanded information and seeks a protective order asserting that her journal entries were posted as a method of catharsis to help her cope with her injuries and were not intended as a communication. Her counsel argues that their production would violate Peggy's right to privacy.

Peggy's battle to keep her MyFazer page private did not end there. INC quickly became suspicious of her "injury" and began an internal investigation into her work station Internet use, including reviewing her password-protected MyFazer page. Peggy did not realize that because she was using her INC computer to access her MyFazer page, INC was able to access the page.

### The Arguments on Both Sides

Does Peggy have a reasonable expectation that she can protect the content of her MyFazer page from discovery by the trampoline manufacturer's counsel? Did INC violate Peggy's right to privacy by accessing her MyFazer page without her permission? If the sought information is discoverable, can it be admissible as evidence?

The answers to these questions lie in the largely unchartered legal territory of social networking sites in which standards of privacy have not yet been defined or adequately tested. This article explores a social networking site user's right to privacy, an adversary's right to obtain information from that site, and the admissibility of the information.

Before asserting an invasion of privacy claim as against her employer, Peggy's counsel should check whether INC had a publicized policy that INC's employees have no privacy interest in any materials created or accessed on company computers. With such a policy in place, an employer generally can review with impunity an employee's activities on the company's computer system. Even if Peggy's MyFazer page is "password-protected," INC may be able to access it if the company's Web browser memorizes users' passwords so that each time Peggy logged onto her MyFazer page from work, she did not have to enter her password. By using INC's computer to access her MyFazer account, Peggy unknowingly granted INC full access to it, and, in so doing, arguably waived any right to privacy in the content therein that she may otherwise have possessed.

Whether the trampoline manufacturer can obtain information from Peggy's MyFazer page is less certain because specific rules governing the discoverability of on-line personal information have not kept pace with new opportunities for online expression, which are being developed faster than regulations can be revised or promulgated.

Because traditional tort law does not recognize invasions of privacy that occur in public, arguments that information posted on social networking sites should not be discoverable because it is "private" face an uphill battle. To determine whether a litigant has an expectation of privacy in an Internet posting, courts will generally first ask whether the person had a "subjective expectation of privacy." In trying to prove a subjective expectation of privacy in a user's profile,

---

**Ronald J. Levine**, a member of this newsletter's Board of Editors, is a litigation partner, and **Susan L. Swatski-Lebson** is a litigation associate, with Herrick, Feinstein LLP, with offices in New York, Newark and Princeton, NJ. Mr. Levine, who co-chairs the firm's Litigation Department, can be contacted at rlevine@herrick.com and Ms. Swatski-Lebson can be contacted at sswatski@her rick.com; Phone: 212-592-1400.

the inherent nature of the profile or its everyday use works against any notion of an expectation of privacy.

Users of such sites "logically lack a legitimate expectation of privacy in the materials intended for publication or public posting." *Steven Guest et al. v. Simon L. Leis et al.*, 255 F.3d 325 (6th Cir. 2001). For this reason, "e-mail messages are afforded more privacy than similar messages on the Internet." *United States v. James A. Maxwell, Jr. et al.*, 45 M.J. 406 (C.A.A.F. 1996). By providing personal information for others to see on a social networking site, a user is not seeking to preserve this information as private, but rather is making a conscious choice to publicize it. To prove a subjective expectation of privacy, users have to first overcome the inherent assumption that they intended to publicize their information. To attempt to overcome that assumption, a user may argue that he/she restricted the privacy settings on the site only to allow those whom he/she accepted as "friends" to view it. Generally, to restrict access, the user must actively change the site's settings. This active step may show the requisite intent to keep the posted information private. However, whether taking this step overcomes the presumption that a user who posts personal information on a Web page can have a reasonable expectation that that information will remain private is questionable.

The United States District Court of New Jersey set the limits of a person's reasonable expectation of privacy at the point where content on a Web page is shared with other people. In the consolidated cases *Beye v. Horizon*,, 06-Civ.-5337 (D. N.J. filed 2006), and *Foley v. Horizon*, 06-Civ.-6219 (D. N.J. filed Dec. 26, 2006) (litigation involving an insurer's refusal to pay health benefits for children's eating disorders), the court ordered the plaintiffs to turn over the children's e-mails, diaries and other writings that were "shared with other people" about their eating disorders, including entries on Web sites such as Facebook or MySpace. The court's proclivity for ordering production of on-line personal information emphasizes both the idea of individual responsibility when using social networking sites and a lowered expectation of privacy where the person asserting a right to privacy is the same person who made the information public in the first place.

This is not to say, however, that a request for production will always prevail. A New Jersey Superior Court denied a request for access to a plaintiff's MySpace and FaceBook sites when a township's school board asked for the disclosure in a student's suit seeking emotional distress damages. *T.V. v. Union Twp. Board of Education*, UNN-L-4479-04 (N.J. Super. Ct. filed Dec. 22, 2004). The court held that the student's privacy interests prevailed absent a particularized showing of relevance, but left open the possibility that ongoing discovery might provide a basis for the court to reconsider its decision. The *United States District Court in Mackelprang v. Fidelity National Title Agency of Nevada, Inc.*, 2007 WL 119149 (D. Nev. Jan. 9, 2007), also left the door open to the possibility of future discovery. In *Mackelprang*, the court denied the defendant's motion to compel production of private messages on the plaintiff's MySpace page, which defense counsel claimed constituted "the same types of electronic and physical relationships she [the plaintiff] characterized as sexual harassment in her Complaint." The court reasoned that "at the time of the request," defense counsel had "nothing more than suspicion or speculation as to what information might be contained in the private messages." However, the court did allow discovery into e-mail messages that would be relevant to assessing the credibility of her emotional distress claims. Notably, nothing in the court's order prevented the defendants from serving discovery requests on the plaintiff demanding production of her MySpace messages that contained information regarding her sexual harassment allegations in the lawsuit or which discussed her alleged emotional distress.

The presumption that a user does not have a reasonable expectation of privacy to information posted on a social networking site is strengthened by the fact that the privacy policies of some of the most popular social networking sites generally disclaim responsibility for circumvention of privacy measures and state that by posting on their site, the user grants the networking site the right to access or disclose the user's content for a variety of purposes. In fact, Facebook's policy actually states, "[p]lease keep in mind that if you disclose personal information [on your page] … this information may become publicly available." http://www.facebook.com/policy.php. Since these sites' privacy policies recognize and even caution that any posted information may become public, a user may not be able to contend reasonably that such information is private and in the case of litigation, non-discoverable.

## Making Information Discoverable

Given the increasing prominence of social networking sites, defense counsel for a manufacturer should consider the following practice tips at the inception of discovery:

1. Search (through Google or similar search engine)individual plaintiffs and key witnesses ("Key Players") to discover their Internet activities.
2. Demand that Key Players identify their e-mail accounts.
3. Investigate whether and which Key Players have or are users of social networking sites:
   a. If any have or are users of a social networking site,
      (1) demand to view it; and
      (2) analyze the relevance of its content.
   b. If relevant,
      (1) demand that the relevant content be produced; and
      (2) the site be preserved.
   c. Production may depend upon:

(1) whether the site is password protected;
(2) who has access to the site;
(3) when the site was created and last edited;
(4) the function or nature of the site; and
(5) whether the entries were created for the purpose of sharing them with others.

4. Resolve disputes regarding privilege:
   a. stipulate that any allegedly "private" content produced will be subject to a protective order to protect the privacy interests of the parties and to prevent disclosure of information to persons having no involvement in the litigation; and/or
   b. seek in camera review of the content at issue and be prepared to demonstrate the need for the information sought by explaining how the on-line entries could shed light on the cause of an injury and/or provide relevant insight into the Key Players' lifestyles that may bear on the case.

## Making Information Admissible

Once information is deemed to be discoverable, the issue becomes whether it is admissible as evidence. Courts weighing the admissibility of Web site postings, e-mail and instant messages are generally holding that these communications can be admissible provided the following two conditions are met. First, unless they are admissions or are subject to another exception, the content cannot be offered for the truth of the matter asserted. This is because website postings are considered out of court statements; thus, they may be subject to a hearsay objection. Second, the proponent must offer direct or circumstantial evidence as to the content's authenticity.

Authentication objections arise because it is possible to create a webpage on a social networking site in another person's name or to send an e-mail or post a message in another's name. Therefore, it is difficult to show who actually is responsible for creating material on the Internet. Discussing the evidentiary standards for evaluating such evidence, a Pennsylvania appellate court wrote that "[w]e see no justification for constructing unique rules for admissibility of electronic communications such as instant messages; they are to be evaluated on a case-by-case basis as any other document to determine whether or not there has been an adequate foundational showing of their relevance and authenticity." *In the Interest of: F.P.*, 878 A.2d 91 (Pa. Super. Ct. 2005). Federal Rule of Evidence 901(b)(4), which is primarily concerned with authentication on the basis of circumstantial evidence, "is one of the most frequently used [Rules] to authenticate e-mail and other electronic records," including the content of Web sites. *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007). Application of the Federal Rules of Evidence to electronic information, however, is not well settled and courts vary in how they weigh whether evidence is sufficient to support a finding of authenticity.

Practice points regarding authenticating content from a Web page include:

- Provide testimony from the person who obtained the copy of the Web page, stating when and how it was copied and affirming that the copy is accurate;
- Subpoena documentation directly from the social networking site provider; and
- Offer evidence that the purported author of a webpage actually wrote it. The normal methods of proving authorship apply to Internet material and include:

1. an admission by the author;
2. testimony of a witness who assisted or observed the creation of the Web page;
3. evidence of similarities between the contested Web page and an authenticated Web page;
4. content on the Web page that connects it the author; and
5. stipulation.

## Conclusion

In sum, the trends in court decisions regarding the discoverability and admissibility of information located on a social networking site do not bode well for Peggy. Since she posted information about herself and her misadventures on the trampoline to her MyFazer page, her counsel will surely face an uphill battle to prevent its production. The moral of the story for Peggy is the same for all users of social networking sites. Although these sites provide users with a sense of intimacy and community, they also create a potentially permanent record of personal information that becomes a virtual information bonanza about a litigant's private life and state of mind. The converse thus becomes the moral for litigation counsel — this new generational fount of potentially discoverable information should be high on the list of priorities when evaluating a new matter.